**PATENT**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | | |
|---|---|---|---|
| In re the application of: | **Daniell, et al.** | | |
| Serial No.: | 09/759,932 | Art Unit: | 2131 |
| Filed: | January 12, 2001 | Examiner: | Arani, Taghi T. |
| For: | SYSTEM AND METHOD FOR PROTECTING A SECURITY PROFILE OF A COMPUTER SYSTEM | Docket No.: | 10004557-1 |

## APPEAL BRIEF UNDER 37 C.F.R. §1.192

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. §1.192 is submitted in support of the Notice of Appeal filed June 6, 2005, responding to the final Office Action of March 9, 2005.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those which may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required therefor (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Company Deposit Account No. 08-2025.

**Certificate of Mailing**

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope, with sufficient postage, addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 20231 on

8-8-05

Signature: Shana R. East

## I. REAL PARTY IN INTEREST

The real party in interest of the instant application is the assignee, Hewlett-Packard Development Company, L.P.

## II. RELATED APPEALS AND INTERFERENCES

There are no known related appeals and interferences that will affect or be affected by a decision in this appeal.

## III. STATUS OF THE CLAIMS

Claims 1-24 are pending in the present application. The final Office Action of March 9, 2005, rejected claims 1, 3-5, 7, 8, and 10-23 under 35 U.S.C. §102 as allegedly anticipated by *Pereira* (U.S. Patent No. 5,809,230). The final Office Action also rejected claims 2, 6, 9, and 24 under 35 U.S.C. §103 as allegedly unpatentable over *Pereira* in view of *Proctor* (U.S. Patent No. 6,530,024).

## IV. STATUS OF AMENDMENTS

No amendments have been made or requested since the mailing of the final Office Action. A copy of the current claims is attached hereto as Appendix A.

## V. SUMMARY OF CLAIMED SUBJECT MATTER

A computer system (e.g., reference numeral 50) of some embodiments comprises memory (e.g., reference numeral 18) and a security application (e.g., reference numeral 52). The security application is configured to display a list of security rules to a user (e.g., page 14, lines 18-19) and to enable ones of the security rules based on user inputs (e.g., page 14, line 23, through page 15, line 2). The security application is configured to lock down resources of the computer system by modifying security settings of the computer system based on which of the security rules are enabled when an activation request is received by the computer system (e.g., page 15, lines 12-18). The security application is configured to store, in the memory, data indicative of the security settings (e.g., page 15, lines 19-22). The security application is configured to perform comparisons between the data and the security settings and to determine when one of the security settings has changed from a first value to another value based on one of the comparisons (e.g., page 16, lines 15-21). The security application is further configured to change the one security setting to the first value in response to the one comparison (e.g., page 16, line 21, through page 17, line 3).

In at least some embodiments, the security application is further configured to transmit a message indicating that the one security setting has changed in response to the one comparison (e.g., page 17, lines 4-15).

## VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 3-5, 7, 8, and 10-23 are rejected under 35 U.S.C. §102 as allegedly anticipated by *Pereira* (U.S. Patent No. 5,809,230).

Claims 2, 6, 9, and 24 are rejected under 35 U.S.C. §103 as allegedly unpatentable over *Pereira* in view of *Proctor* (U.S. Patent No. 6,530,024).

## VII. ARGUMENT

A proper rejection of a claim under 35 U.S.C. §102 requires that a single prior art reference disclose each element of the claim. See, *e.g.*, *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 U.S.P.Q. 303, 313 (Fed. Cir. 1983). In addition, "(t)he PTO has the burden under section 103 to establish a *prima facie* case of obviousness. It can satisfy this burden only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references." *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988) (citations omitted).

**Discussion of Advisory Action**

In the Advisory Action of May 31, 2005, it is asserted that:

> "(t)he Applicant's arguments relating to security application detection of an unauthorized change of security setting and a change of said security setting in response to a detection of an unauthorized change of the security setting in contrast with the cited prior art of resetting executable security components (not values as argued) would require further consideration and/or search."

If amendments are presented after a final rejection, then it is proper for the Patent Office to refuse to enter such amendments if they "require further consideration and/or search." However, Applicants have presented no amendments after a final rejection. Moreover, it is improper for the Patent Office to refuse to consider an applicant's arguments after final rejection on the grounds that such arguments allegedly "require further consideration and/or search." Thus, if Applicants' arguments in the instant case show that the rejections set forth in the final Office Action are improper, then the rejections

should be withdrawn regardless of whether "further consideration and/or search" is required.

In addition, it is further asserted in the Advisory Action that "Applicant's withholding of copending applications Serial No. 09/759,428, 09/760,236 and 09/760,404 has also raised possible double patenting issues in the case." Applicants observe that each of the foregoing patent applications has yet to issue into a patent and are, therefore, still pending. Accordingly, it is impossible for these applications to raise double patenting issues that could preclude patentability of the instant application. In this regard, M.P.E.P. §804(I)(B) states that a patent application is to be allowed to issue into a patent when it is otherwise in a condition for allowance even if there are double patenting issues between the application and another pending patent application. Therefore, the Patent Office does not need to evaluate any possible double patenting issues between the instant application and any of the cited pending patent applications in order to allow the instant application to issue into a patent. Moreover, for at least the reasons set forth below, Applicants respectfully request that the rejections set forth in the final Office Action be overruled regardless of whether there are any possible double patenting issues between the instant application and the cited pending patent applications.

**Discussion of 35 U.S.C. §102 Rejections of Claims 1, 3-5, 7, 8, and 10-23**

Claim 1 presently stands rejected in the final Office Action under 35 U.S.C. §102 as allegedly anticipated by *Pereira* (U.S. Patent No. 5,809,230). Claims 5, 8, and 20 comprise similar claimed limitations which are missing from *Pereira* (with respect to the outstanding 35 U.S.C. §102 rejections) as claim 1. Claims 3, 4, 7, 10-18, and 21-23 depend from a respective

one of the claims 1, 5, 8, and 20. Therefore, claim 1 is discussed below as an exemplary claim for discussion.

Claim 1 presently reads as follows:

> 1. A computer system, comprising:
> memory; and
> a security application configured display a list of security rules to a user and to enable ones of said security rules based on user inputs, said security application configured to lock down resources of said computer system by modifying security settings of said computer system based on which of said security rules are enabled when an activation request is received by said computer system, said security application configured to store, in said memory, data indicative of said security settings, ***said security application configured to perform comparisons between said data and said security settings and to determine when one of said security settings has changed from a first value to another value based on one of said comparisons, said security application further configured to change said one security setting to said first value in response to said one comparison***. (Emphasis added).

Applicants respectfully assert that the cited art fails to disclose at least the features of claim 1 highlighted hereinabove. Thus, the 35 U.S.C. §102 rejection of claim 1 is improper.

In this regard, it is asserted in the final Office Action that *Pereira* teaches:

> "said security application configured to perform comparisons between said data and said security settings and to determine when one of said security settings has changed from a first value to another value based on once of said comparisons, said security application further configured to change said one security setting to said first value in response to said one comparison (column 10, lines 64-column 11, line 6)."

The cited section of *Pereira* appears to describe an "access control program" that restricts the use of resources within a computer system. However, Applicants respectfully assert that the "access control program" does not appear to include a "security setting."

In particular, *Pereira* appears to teach that an "access control program" is segmented into three components, and each component verifies that the other components are "loaded and are operational." See column 10, lines 48-67. Further, all three program components are apparently reloaded if any of the program components detects that the other program

components have been changed. See column 11, lines 1-5. However, none of the program components appear to include a "security setting," as described by claim 1. In this regard, the program components appear to be executable computer code that uses various settings ***stored in external data files*** to protect the resources of a computer system. See column 9, lines 44-48. Thus, the detection of a modified program component and subsequent reloading of the program component in *Pereira* does not and cannot constitute a determination of "when one of said security settings has changed...based on one of said comparisons" and a change of "said one security setting... in response to said one comparison," as described by claim 1.

For at least the above reasons, Applicants respectfully assert that *Pereira* fails to disclose each feature of claim 1. Accordingly, the 35 U.S.C. §102 rejection of claim 1 should be overruled.

**Discussion of 35 U.S.C. §103 Rejections of Claims 2, 6, 9, and 24**

Claims 2, 6, 9, and 24 presently stand rejected in the final Office Action under 35 U.S.C. §103 as allegedly unpatentable over *Pereira* in view of *Proctor* (U.S. Patent No. 6,530,024). However, Applicants respectfully assert that the combination of *Pereira* and *Proctor* is improper.

In this regard, the final Office Action alleges that it would have been obvious to combine *Pereira* and *Proctor* without providing a cite to ***any*** reference in the cited art for establishing a reason or motivation to combine the teachings of *Pereira* with the teachings of *Proctor*. The final Office Action, therefore, fails to establish that it would have been obvious to one of ordinary skill in the art to combine such teachings. "There must be some reason, suggestion, or motivation ***in the prior art*** whereby a person of ordinary skill in the field of the invention would make the combination." *In re Oetiker*, 977 F.2d 1443, 1447, 24 U.S.P.Q.2d

1443 (Fed. Cir. 1992) (emphasis added). "Our case law makes clear that the best defense against the subtle but powerful attraction of a hindsight-based obviousness analysis is rigorous application of the requirement for a showing of the teaching or motivation to combine prior art references." *In re Dembiczcak*, 175 F.3d 994, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999).

For at least the above reasons, Applicants respectfully assert that the final Office Action fails to establish a *prima facie* case of obviousness with respect to the claims rejected in view of the alleged combination of *Pereira* and *Proctor*. Accordingly, the 35 U.S.C. §103 rejections of claims 2, 6, 9, and 24 should be overruled.

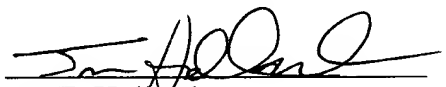
In addition, claims 2, 6, 9, and 24 depend from and, therefore, include all of the limitations of a respective one of the claims 1, 5, 8, and 20. Even if the combination of *Pereira* and *Proctor* is deemed proper, *Proctor* does not suggest the features missing from *Pereira* as described above in the Discussion of 35 U.S.C. §102 Rejections of Claims 1, 3-5, 7, 8, and 10-23. Therefore, the 35 U.S.C. §103 rejections of claims 2, 6, 9, and 24 are improper and should be overruled regardless of whether the alleged combination is deemed to be proper.

## CONCLUSION

Based on the foregoing discussion, Applicants respectfully request that the Examiner's final rejections of claims 1-24 be overruled and withdrawn by the Board, and that the application be allowed to issue as a patent with all pending claims.

Respectfully submitted,

**THOMAS, KAYDEN, HORSTEMEYER & RISLEY, L.L.P.**

By: 

Jon E. Holland
Reg. No. 41,077
(256) 704-3900 Ext. 103

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

## VIII. CLAIMS - APPENDIX

1. A computer system, comprising:

memory; and

a security application configured display a list of security rules to a user and to enable ones of said security rules based on user inputs, said security application configured to lock down resources of said computer system by modifying security settings of said computer system based on which of said security rules are enabled when an activation request is received by said computer system, said security application configured to store, in said memory, data indicative of said security settings, said security application configured to perform comparisons between said data and said security settings and to determine when one of said security settings has changed from a first value to another value based on one of said comparisons, said security application further configured to change said one security setting to said first value in response to said one comparison.

2. The system of claim 1, wherein said security application is further configured to transmit a message indicating that said one security setting has changed in response to said one comparison.

3. The system of claim 1, wherein said security application is further configured to store said data in response to said activation request.

4. The system of claim 1, wherein said security application is further configured to periodically compare each of said security settings to said data.

5. A system for locking down resources of computer systems, comprising:

means for receiving a request for activating a security profile;

means for modifying security settings of a computer system in response to said request;

means for storing data indicative of said modified security settings;

means for automatically determining when one of said security settings has changed from a first value to another value by periodically comparing said data to said security settings; and

means for automatically changing said one security setting to said first value in response to a determination by said determining means that said one security setting has changed.

6. The system of claim 5, wherein said system further comprises:

means for automatically transmitting, in response to said determination, a message indicating that said one setting has changed.

7. The system of claim 5, wherein said storing means is configured to store said data in response to said request.

8. A method for locking down resources of computer systems, comprising:

receiving a request for activating a security profile;

modifying security settings of a computer system in response to said request;

storing data indicative of said security settings, as modified by said modifying;

automatically determining when one of said security settings has changed from a first value to another value by periodically comparing said data to said security settings; and

automatically changing said one security setting to said first value in response to a determination in said determining that said one security setting has changed.

9. The method of claim 8, further comprising:

automatically transmitting, in response to said determination, a message indicating that said one security setting has changed.

10. The method of claim 8, wherein said storing is performed in response to said request.

11. The system of claim 1, wherein said security application is configured to change said one security setting in response to said one comparison without changing another of said security settings in response to said one comparison.

12. The system of claim 1, further comprising an operating system configured to analyze said one security setting to determine whether access to a resource of said computer system is restricted.

13. The computer system of claim 12, wherein said one security setting is associated with one of said security rules, and wherein said operating system is configured to enforce said one security rule based on said one security setting.

14. The computer system of claim 13, wherein said security application is not configured to enforce said one security rule.

15. The computer system of claim 12, wherein said security settings are within a machine state analyzed by said operating system for selectively enforcing said security rules.

16. The computer system of claim 15, wherein said data is separate from said machine state and is stored in said memory by said security application in response to said activation request.

17. The computer system of claim 16, wherein said one security setting is a flag associated with said resource.

18. The system of claim 5, further comprising an operating system configured to analyze said one security setting to determine whether access to a resource of a computer system is restricted.

19. The method of claim 8, wherein said one security setting is analyzed by an operating system of said computer system in order to control access to a resource of said computer system.

20. A computer system, comprising:

memory;

an operating system configured to analyze a machine state to control operation of said computer system, said machine state including a security setting associated with a resource of said computer system and indicating whether access to said resource is restricted, wherein said operating system is configured to analyze said security setting to control access to said resource; and

a security application configured to modify said security setting based on a user input and to store, in said memory, data indicative of a state of said security setting, as modified by said security application, said security application configured to perform a comparison between said data and said security setting to detect an unauthorized change of said security setting, said security application further configured to automatically change said security setting based on said data in response to a detection of an unauthorized change of said security setting.

21. The computer system of claim 20, wherein said security application is configured to set said security setting based on said user input in response to a user activation request.

22. The computer system of claim 21, wherein said security application is configured to store said data in said memory in response to said user activation request.

23. The computer system of claim 20, wherein said security setting is a flag stored within a register.

24. The computer system of claim 20, wherein said security application is further configured to transmit, in response to said detection, a message indicating that said one security setting has changed.

## IX. EVIDENCE - APPENDIX

None.

## X. RELATED PROCEEDINGS - APPENDIX

None.

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10004557-1

AF

RPW



**IN THE**
**UNITED STATES PATENT AND TRADEMARK OFFICE**

**Inventor(s):** Daniell, et al.

**Confirmation No.:** 2759

**Application No.:** 09/759,932

**Examiner:** Arani, Taghi T.

**Filing Date:** 01/12/2001

**Group Art Unit:** 2131

**Title:** SYSTEM AND METHOD FOR PROTECTING A SECURITY PROFILE OF A COMPUTER SYSTEM

**Mail Stop Appeal Brief-Patents**
**Commissioner For Patents**
**PO Box 1450**
**Alexandria, VA 22313-1450**

**TRANSMITTAL OF APPEAL BRIEF**

**Sir:**

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on **June 6, 2005**.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

**(complete (a) or (b) as applicable)**

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

( ) (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

| | | |
|---|---|---|
| ( ) | one month | $120.00 |
| ( ) | two months | $450.00 |
| ( ) | three months | $1020.00 |
| ( ) | four months | $1590.00 |

( ) The extension fee has already been filled in this application.

(X) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account **08-2025** the sum of **$500.00**. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

(X) I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450. Date of Deposit: **8/8/2005**

OR

( ) I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number_____ on _____

Number of pages:

Typed Name: **Shana L. East**

Signature: Shana L. East

Respectfully submitted,

**Daniell, et al.**

By _____

**Jon E. Holland**

Attorney/Agent for Applicant(s)
Reg. No. **41,077**

Date: **8/8/2005**

Telephone No.: **(256) 704-3900**